

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO**

PHILIPS MEDICAL SYSTEMS PUERTO
RICO, INC.,

Plaintiff,

v.

GIS PARTNERS CORP.; HERNAN
TORO; DAVID SUMPTER and RADAMES
BRACERO,

Defendants.

CIVIL No.

RE: PRELIMINARY AND PERMANENT
INJUNCTIVE RELIEF PURSUANT TO THE
COMPUTER FRAUD AND ABUSE ACT, 18
U.S.C. §1030, PUERTO RICO'S
INDUSTRIAL AND TRADE SECRET
PROTECTION ACT, 10 P.R. LAWS ANN.
§§4131-4141; BREACH OF CONTRACT;
UNFAIR COMPETITION; UNJUST
ENRICHMENT AND DEMAND FOR JURY
TRIAL

**MEMORANDUM OF LAW IN SUPPORT OF
PRELIMINARY INJUNCTION**

TO THE HONORABLE COURT:

COMES NOW plaintiff, Philips Medical Systems Puerto Rico, Inc. ("Philips PR" or "plaintiff"), through its undersigned attorneys and, pursuant to Fed. R. Civ. P. 65(a), respectfully submits the instant memorandum in support of its request for the issuance of a preliminary injunction to enjoin GIS Partners Corp. ("GIS"), Hernán Toro-Aponte ("Mr. Toro Aponte"), David Sumpter López ("Mr. Sumpter López") and Radames Bracero ("Mr. Bracero")(hereinafter jointly referred to as "defendants") from accessing plaintiff's CSIP Digital Rights Management Application and Proprietary Service Applications¹ without authorization; trafficking their passwords and other security features and using its trade secrets for their own profit and financial benefit.

¹ Alike in its Complaint, plaintiff's Proprietary Service Applications and CSIP Digital Rights Management Application are at times jointly referred to as "proprietary computer systems".

PRELIMINARY STATEMENT AND FACTUAL SUMMARY

On even date, plaintiff has filed a Complaint for preliminary and permanent injunctive relief arising under the Computer Fraud and Abuse Act, 18 U.S.C. §1030 (“CFAA”) and Puerto Rico’s Industrial and Trade Secret Protection Act, 10 P.R. Laws Ann. §§4131-4141 (“ITSPA”), among other remedies. Philips PR is seeking injunctive relief as a result of defendants’ unauthorized access of plaintiff’s protected computer systems and unlawful trafficking of passwords in violation of the CFAA, and trade secrets misappropriation in violation of ITSPA.

As fully described in plaintiff’s Complaint, Philips PR is a corporation organized and existing under the laws of the Commonwealth of Puerto Rico, engaged, among other things, in the sale and servicing of medical equipment and supplies. As part of its trade, Philips PR provides for the repair and maintenance of its products through authorized field service engineers (“Field Service Engineer(s)”) and/or agents with accredited access to their internal computer systems protected by passwords and other security features. Philips PR is a subsidiary of Royal Philips Electronics (hereinafter, collectively referred to as “Philips”).

In connection with the installation, configuration, maintenance and repair of Philips medical equipments, plaintiff utilizes certain Proprietary Service Applications – including, but not limited to software, hardware and codes – not available for sale or licensing to customers or third parties. These Proprietary Service Applications interconnect and communicate with Philips’ CSIP Digital Rights Management Application embedded on each of the systems it manufactures. Philips’ CSIP Digital Rights Management Application, in turn, controls third party access and use of protected digital information, files and other restricted content within its medical equipments.

Any access to or use of Philips' Proprietary Service Applications by anyone other than authorized Philips personnel is strictly prohibited. Moreover, alike Philips' CSIP Digital Rights Management Application, Proprietary Service Applications are protected by passwords and other security features including, but not limited to, its Field Service Engineers' login credentials.

Co-defendants Mr. Toro Aponte, Mr. Sumpter López and Mr. Bracero, as former employees of Philips PR, had access to plaintiff's proprietary computer systems and confidential information. During their employment, however, the former employees entered into an Employee Ethics and Intellectual Property Agreement ("*Confidentiality Agreements*") pursuant to which they agreed to keep confidential and not to disclose or use any secret or confidential (proprietary) information belonging to plaintiff either during or after employment. Therefore, and as acknowledged by defendants, Philips' proprietary computer systems and all information contained therein were – and continue to be – the exclusive property of Philips PR.

Still, and unbeknownst to Philips PR, at the time or prior to his termination of employment, Mr. Bracero unlawfully extracted and retained copies of Philips' Proprietary Service Applications to somehow manipulate and gain access to Philips' CSIP Digital Rights Management Application for defendants' own profit and financial benefit. Moreover, and in order to fulfill said purpose, Mr. Bracero facilitated defendants' access to plaintiff's proprietary computer systems by clandestinely disclosing to GIS, Mr. Sumpter-López and/or Mr. Toro-Aponte its passwords, security features and other related confidential information. Upon information and belief, at the time of filing the instant Complaint

defendants continue to access Philips' proprietary computer systems without authorization, with the latest unauthorized access having occurred on August 18, 2015.

Clearly, defendants' actions are in violation of CFAA and ITSPA, and, unless enjoined, threaten to cause plaintiff irreparable injuries such as the loss of customers, both potential and actual; loss of goodwill; loss of competitive advantage; and the dilution of the value of its rights/confidential information. As a result, Philips PR has been forced to bring this action to stop defendants from further using its Proprietary Service Applications for accessing its CSIP Digital Rights Management Application without authorization and to enjoin them from further misappropriating its trade secrets and causing it irreparable harm.

RELIEF SOUGHT IS MANDATED BY STATUTE AND COMMON LAW

Under the facts described in Philips PR's Complaint, the Court should issue an injunction on statutory grounds. Generally, in an action for a statutory injunction, once a violation has been demonstrated, the moving party need only show that there is a reasonable likelihood of future violations in order to obtain relief. See Century ML Bable Corp. v. Carrillo Díaz, 43 F.Supp.2d 166, 171-172 (D.P.R. 1998); see also CoxCom, Inc. v. Chaffee, 536 F.3d 101, n.14 (1st Cir. 2008). The preliminary injunction relief requested by Philips PR is expressly authorized by the two (2) statutes implicated by defendants' conduct. See 18 U.S.C. §1030(g) (CFAA provides for "injunctive or other equitable relief"); 10 P.R. Laws Ann. §4136 ("In all cases in which it is proven that an industrial or trade secret has been misappropriated, the court may issue a preliminary injunction order, for which the plaintiff shall not be under the obligation to prove irreparable damages").

Additionally and alternatively, Rule 65 authorizes this Court to issue a preliminary injunction based on plaintiff's showing that: (1) it is likely to succeed on the merits; (2) it will suffer irreparable harm if an injunction is not issued; (3) it lacks an adequate remedy at law; (4) the balance of harms tips in favor of Philips PR; and (5) the public interest favors injunctive relief. See Century ML Cable Corp., *supra* at 172; see also American Health, Inc. v. Chevere, 2013 WL 5297295, *5-6 (D.P.R. 2013); Vaquería Tres Monjitas, Inc. v. Irizarry, et. al., 587 F.3d 464, 482-483 (1st Cir. 2009); Borinquen Biscuit Corp. v. M.V. Trading Corp., 443 F.3d 112, 115 (1st Cir. 2006). This Court is to apply a "sliding scale" in evaluating these elements. See Braintree Laboratories, Inc. v. Citigroup Global Markets, Inc., 622 F.3d 36, 42 (1st Cir. 2010); Total Petroleum Puerto Rico Corp. v. Colón-Colón, 577 F.Supp.2d 537, 551 (D.P.R. 2008) ("Evaluating irreparable harm and its likelihood of success on the merits must be considered together. The greater the likelihood of success on the merits, the less required showing of irreparable harm."); Telerep Caribe, Inc. v. Zambrano, 146 F.Supp.2d 134, 145 (D.P.R. 2001); LaCoste Alligator, S.A. v. Santiago, 2006 WL 1047030, *4 (D.P.R. 2006); Camilo v. Nieves, 792 F.Supp.2d 232, 238-239 (D.P.R. 2011); Ross-Simons of Warwick, Inc. v. Baccarat, Inc., 102 F.3d 12, 19 (1st Cir. 1996); Borinquen Biscuit Corp., *supra* at 115. Particularly in view of the fact that there is a significant likelihood that defendants will continue accessing plaintiff's CSIP Digital Rights Management Application and Proprietary Service Applications without authorization;² trafficking their passwords and other security features and using its trade secrets for their own profit and financial benefit in the absence of injunctive relief. As further explained below, Philips PR does not

² See e.g. In Re America Online, Inc., 168 F.Supp.2d 1359 (concluding that phrase "without authorization" in the CFAA "contemplate[s] a situation where an outsider, or someone without authorization, accesses a computer"); see also Lisa J. Sotto, Privacy and Data Security Law Deskbook, §13.03[B] (Wolters Kluwer 1st ed. 2010).

have an adequate remedy at law for its ongoing injuries and will suffer irreparable harm if injunctive relief is not granted.

A. Likelihood of Success on the Merits

1. Defendants' Conduct Is In Violation Of The CFAA.

In this case, for the reasons that follow, Philips PR has demonstrated a likelihood of succeeding on the merits on its civil claim under the CFAA given defendants' blatant violations of applicable federal and state law. First, Philips PR's proprietary computer systems are "protected computers" within the meaning of Section 1030(e)(2)(B) of the CFAA, as they are "used in or affecting interstate or foreign commerce or communication". 18 U.S.C. §1030(e)(2)(B); see also Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals, 147 (IAPP 2013)("Due to this broad definition, the Act generally will apply to any computer connected to the Internet"); Susan W. Brenner, Data Security and Privacy Law, 2 Data Sec. & Privacy Law §15:7 (2015)("As a result of the 1996 amendment, the statute now reaches conduct directed at any computer connected to the Internet, regardless of whether the computers involved are located in the same state"); Continental Group, Inc. v. KW Property Management, LLC, 622 F.Supp.2d 1357, 1370 (S.D. Fla. 2009); Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 248 F.R.D. 598, 602 and n.5 (D. Kan. 2008). Philips' proprietary computer systems are connected to the Internet and only made available to authorized Philips PR Field Service Engineers; which, at the time of employment with plaintiff, are required to enter into confidentiality/non-disclosure agreements pursuant to which they agree not to disclose, in whole or in part, and/or by any means whatsoever, Philips' proprietary information and trade secrets. See Complaint, ¶¶11, 19-22, 27, 51, 57, 77; see also NCMIC Fin. Corp. v. Artino, 638 F.Supp.2d 1042, 1060 (S.D.

Iowa 2009)(stating that the “protected computer” element was established where the computers at issue were connected to the Internet); Merritt Hawkins & Assocs., LLC v. Gresham, 948 F.Supp.2d 671, 674 (N.D. Tex. 2013)(stating that “[p]leading specific facts that the defendant accessed a computer connected to the Internet is sufficient to establish that the accessed computer was ‘protected’”).

Second, Philips PR has sufficiently demonstrated that defendants have, intentionally and without authorization, manipulated Philips’ Proprietary Service Applications to obtain access to CSIP Digital Rights Management Application in violation of 18 U.S.C. §§1030(a)(2)(C) and (a)(5)(B). See Complaint, ¶¶6-9, 23, 47-50, 52, 56-63, 65-74. Because users must have an active and authorized Philips’ IST/PMSec account in order to run and/or obtain a valid response from Philips’ CSIP Digital Rights Management Application,³ unauthorized users cannot access plaintiff’s proprietary computer systems without taking affirmative steps to circumvent those security measures. See Complaint, ¶¶19 and 50. Indeed, defendants’ conduct is without authorization, in that they have obtained information as outsiders – i.e. unauthorized users – for their own profit and financial benefit by intentionally accessing a protected computer without approval and, in doing so, have impaired the integrity of plaintiff’s proprietary computer systems, including their data. See 18 U.S.C. §§1030(a)(2)(C) and (a)(5)(B); see also U.S. v. Morris, 928 F.2d 504, 508 (2nd Cir. 1991)(concluding that, pursuant to the Senate Report’s discussion, subsection 1030(a)(5) was designed to target “outsiders”).

Beyond that, there can be no question that defendants’ acts of unauthorized infiltration, illegal copying and dissemination – i.e. trafficking – of Philips’ proprietary

computer systems, along with their passwords and other security features, have caused and will continue to cause damage within the meaning of Section 1030(e)(8) of the CFAA, inasmuch as they have substantially impaired their integrity in an amount in excess of \$5,000.00. More specifically, defendants' alteration of plaintiff's Proprietary Service Applications to somehow gain access to its CSIP Digital Rights Management Application for their personal benefit not only undermines the accuracy, consistency, quality and overall completeness of plaintiffs' proprietary computer systems developed internally for commercial purposes, but also has a negative effect on its normal business operations by diminishing the usability of Philips' information and systems. Section 1030(3)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information".

Accordingly, defendants' actions of depriving plaintiff of the means to control the quality and availability of its proprietary computer systems clearly satisfy the CFAA's "damage" requirement. See also Complaint, ¶¶56-63, 65-74.

Lastly, defendants' actions have also caused Philips PR to incur "loss" as said term is defined by the CFAA. Pursuant to Section 1030(e)(11) "loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service". 18 U.S.C. §1030(e)(11); see also EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001)(holding that "Congress intended the term 'loss' to target remedial expenses borne by the victims that could not properly be considered direct

³ See Complaint, ¶¶14-15. PMSec ("Philips Medical Systems Security") is a proprietary legacy platform/solution for Philips' CSIP Digital Rights Management Application. In turn, IST ("Integrated Security

damage caused by a computer hacker”); A.V. v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2012); SuccessFactors, Inc. v. Softscape, Inc., 544 F.Supp.2d 975, 980-981 (N.D. Cal. 2008)(holding that the cost of investigating and identifying the CFAA offense, including “many hours of valuable time away from day-to-day responsibilities, causing losses well in excess of \$5,000” qualified as “cost[s] of responding to an offense” under §1030(e)(11)). To be sure, as set forth in plaintiff’s Complaint, Philips PR has already spent well in excess of \$5,000.00 investigating⁴ and assessing – in conjunction with outside forensic experts – the possible impairment to the integrity of its protected computer systems, taking action to counteract defendants’ theft, and conducting a damage assessment regarding defendant’s unauthorized access. See Complaint, ¶¶49, 58-59, 70-71.

Philips PR is thus likely to prevail on the merits of its CFAA claim.

2. Defendants Are Also Liable Under ITSPA.

In terms of grounds for action, ITSPA provides that “any natural or juridical person who misappropriates a trade secret shall be held accountable for any damages caused to its owner”. See 10 P.R. Laws Ann. §4134. More fundamentally, however, Section 4136 allows for the Court to issue a preliminary injunction order, without the need for showing irreparable harm, “in all cases in which it is proven that an industrial or trade secret has been misappropriated”. Id. at §4136.

As described in its Complaint, Philips PR’s proprietary computer systems, which are not available from public sources and would not have been available to defendants but for Mr. Toro-Aponte’s, Mr. Sumpter López’s and/or Mr. Bracero’s initial access to the same during their employment with Philips PR, contain valuable confidential information

Tool”) is Philips’ existing proprietary platform/solution for its CSIP Digital Rights Management Application.
⁴ See *infra* at n. 5.

belonging to plaintiff. See Complaint, ¶¶10-12, 19, 32, 51, 76-81. Clearly, the absconded proprietary information obtained by defendants is of high commercial value and importance, and is useful to any entity that would compete with Philips PR, if publicized. See Complaint, ¶¶76-81. Nonetheless – and despite the fact that they knew they had no legal rights in and to Philips’ proprietary computer systems – by and through Mr. Bracero, defendants unlawfully extracted and retained copies of Philips’ Proprietary Service Applications to somehow manipulate⁵ and gain access to Philips’ CSIP Digital Rights Management Application and all confidential information contained therein following their employment. See e.g. American Health, Inc., *supra* at *3-4; see also Complaint, ¶¶21, 23, 30-31, 35 and 39.

Each of these items are “trade secrets” as defined in Section 4132.10 P.R. Laws Ann. §4132; see also American Health, Inc., *supra* at *4. In pertinent part, Section 4132 deems “trade secrets” to be “any information: (a) that has a present or a potential independent financial value or that provides a business advantage, insofar as such information is not common knowledge or readily accessible through proper means by persons who could make a monetary profit from the use or disclosure of such information, and (b) for which reasonable security measures have been taken, as circumstances dictate, to maintain its confidentiality”. In addition, an analysis of relevant case law evinces that any distinctive and clearly identifiable information can turn into a trade secret as long as it has some value and has been kept secret. See e.g. Restatement Third, Unfair Competition, §39 (1995); see also

⁵ Although the precise means by which defendants have been able to manipulate Philips’ MR Response Generator Tool without an active and authorized Philips’ IST/PMSec account in order to run and/or obtain a valid response from Philips’ CSIP Digital Rights Management Application is not yet known – and will be the subject of further investigation – the fact remains that all entries to Philips’ proprietary computer systems have not been authorized by plaintiff, are connected to co-defendant Mr. Bracero and GIS, and have been pursued by defendants clandestinely. See Complaint, ¶50.

Positive Report regarding Puerto Rico Bill Senate 1850 (which eventually turned into ITSPA) of November 10, 2011; American Health, Inc., *supra* at *3; Quality Water Service and Distribution Corp. v. Caribbean Water Coolers Inc., 2012 WL 4648299, *5-8 (P.R. Ct. App. Aug. 28, 2012); RKI, Inc. v. Grimes, 177 F.Supp.2d 859, 880 (N.D. Ill. 2001)(granting permanent injunction based upon actual misappropriation of trade secrets); Optos, Inc. v. Topcon Med. Sys., Inc., 777 F.Supp.2d 217, 238-240 (D. Mass 2011).

On the other hand, the above conclusion is further supported by the provisions of the *Confidentiality Agreements* subscribed by co-defendants Mr. Toro Aponte, Mr. Sumpter López and Mr. Bracero, which they agreed to uphold through and following their employment with Philips PR. *See* Complaint, ¶¶30-31, 34 and 39; *see also* Complaint, Exhibits 3-5. Under the terms of each of the *Confidentiality Agreements*, defendants agreed to keep confidential and not to disclose or use any secret or confidential (proprietary) information belonging to plaintiff either during or after employment. *Id.* Moreover, the relevant confidentiality clauses required that defendants return and deliver to plaintiff all secret and confidential (proprietary) information accessed and/or acquired during their employment, and a continued obligation to comply with the same ensuing termination.⁶ *Id.* Hence, defendants knew they were precluded from copying, reproducing, disseminating or using Philips' Proprietary Service Applications; trafficking their passwords and other security features; circumventing plaintiff's security measures to unlawfully access its CSIP Digital Rights Management Application; and/or using its trade secrets for their own profit and financial benefit. *Id.*; *see also* Optos, Inc., *supra* at 239-240.

⁶ Which defendants refused to subscribe at the time of termination. *See* Complaint, ¶¶34 and 39.

Accordingly, Philips PR has alleged and demonstrated a likelihood that it will succeed on its claim under ITSPA. Defendants actions, as outlined, entail “the acquisition of a trade secret belonging to another person who knew or should have known that he/she acquired such secret directly or indirectly through improper means”. See 10 P.R. Laws Ann. §4134(a). More so, given that plaintiff’s proprietary computer systems were developed by it for its own competitive advantage and were implemented using security measures for purposes of limiting the number of individuals with access to such information, defendants’ actions constitute “misappropriation”, as defined by Section 4134 of ITSPA, in that they comprise the “use of a trade secret belonging to another without his/her express or implicit consent, by a person who: (1) Used improper means to gain knowledge of the trade secret, or (2) at the time of disclosure or use, such person knew or should have known that such trade secret was: (A) Obtained through a person who acquired such information through the use of improper means; obtained under the circumstances from which a duty to maintain confidentiality or to limit use ensues; (C) obtained through a person who had the duty-bound to the trade secret’s owner to maintain confidentiality or to limit use”. Id.; see also Complaint, ¶¶10-12, 19, 51, 77, 79.

Philips PR is thus likely to prevail on the merits of its ITSPA claim.

B. No Adequate Remedy at Law

Defendants’ violations of the CFAA and ITSPA have caused, and continue to cause, irreparable damage to Philips PR, which cannot be adequately compensated with money damages. Without a doubt, plaintiff’s ability to attract and retain customers for the repair and maintenance of its products depends on the continued security and integrity of its proprietary computer systems, which allow for conducting tests and diagnostic analyses not

available through public sources. See Complaint, ¶¶51 and 77. As such, plaintiff's irreparable injuries include, but are not limited to: loss of customers, both potential and actual; loss of goodwill; loss of competitive advantage and dilution of the value of its rights/confidential information. See e.g. YourNetDating, LLC v. Mitchell, 88 F.Supp.2d 870, 872 (N.D. Ill. 2000)(granting TRO in CFAA case where the "showing of irreparable harm is in the damage to the goodwill of its services"); Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, 252-253 (S.D.N.Y. 2000)(granting preliminary injunction in CFAA case where irreparable harm could've resulted from the potential substantial loss in business and defendants' use of misappropriated data); Ross-Simons of Warwick, Inc., *supra* at 20 ("By its very nature injury to goodwill and reputation is not easily measured or fully compensable in damages").

In terms of plaintiff's claim under ITSPA, however, plaintiff NEED NOT show irreparable harm to warrant injunctive relief in its favor.⁷ Said lowered burden, though not necessary for the availability of injunctive relief, does not change the fact that under the circumstances – as outlined above and described in its Complaint – Philips PR would still suffer irreparable harm. To be sure, under ITSPA plaintiff need only allege that: (1) it is the rightful owner of a trade secret; (2) that the defendant misappropriated such trade secret; (3) that the disclosure or use thereof by the defendant has caused or has the potential of causing damages to the plaintiff; and (4) that it is likely that the plaintiff will prevail. See 10 P.R. Laws Ann. §§4132, 4134 and 4136; see also e.g. Quality Water Service and Distribution Corp., *supra*. Consequentially, the equitable remedies afforded by ITSPA do not entail alleging or proving at this juncture the set of requirements ordinarily required under the

“ordinary” injunction standards. By itself, however – and as previously discussed – the mere fact that Philips PR’s losses are defendants’ gains merely makes this situation that much worse and the need for injunctive relief that much greater.

Indeed, courts in this Circuit have recognized that the misappropriation of trade secrets/confidential information is irreparable. See e.g. American Health, Inc., supra at *5-6; see also Optos, Inc., supra at 241; TouchPoint Solutions, Inc. v. Eastman Kodak Co., 345 F.Supp.2d 23, 32 (D. Mass. 2004); Picker Int’l Corp. v. Imaging Equip. Servs, Inc., 931 F.Supp. 18, 44 (D. Mass. 1995). Here, the degree of tests and diagnostic analyses being conducted by defendants for the proper maintainability of the Philips equipments located at Medical X Ray Center, P.S.C and Aibonito Mennonite General Hospital could not be undertaken were it not for their breach of plaintiff’s proprietary computer systems. That is, the level of unauthorized access is such that defendants’ process of identifying the real problems that need to be resolved on the machinery being serviced would ultimately be more difficult without access to plaintiff’s proprietary computer systems. Accordingly, if defendants’ entry into plaintiff’s proprietary computer systems is allowed to remain, the loss of Philips PR’s competitive advantage and future business is difficult, if not impossible, to measure fully. Likewise, the loss and/or devaluation of plaintiff’s confidential/trade secret information is an irreparable harm that cannot be remedied by money damages.

The same is true with the substantial loss of business that plaintiff may suffer from defendants’ continued unauthorized access through manipulated and/or circumvented security means. See Complaint, ¶¶23, 50 and 68; see also e.g. Ross-Simons of Warwick, Inc., supra at 18 (“To establish irreparable harm... a plaintiff need not demonstrate that the

⁷ See supra, 10 P.R. Laws Ann. §4136 (“In call cases in which it is proven that an industrial or trade secret has been misappropriated, the court may issue a preliminary injunction order, for which the **plaintiff shall not**

denial of injunctive relief will be fatal to its business”). As outlined in its Complaint, defendants’ servicing of Philips equipment at Medical X Ray Center and Aibonito Mennonite General Hospital rests on their misrepresentation to clients that the equipments’ embedded and protected computers are being access through legitimate means when, in fact, they are not. See Complaint, ¶67. These clients, in turn, attracted by defendants’ “cut-priced” services, continue to use and rely on said work without knowledge that the latter’s “professional assessment” rests on the unauthorized use of plaintiff’s proprietary computer systems. In that respect, there is no accurate telling or measuring of the cognizable threat that naturally arises from the likelihood of defendants usurping other purchasers of Philips medical equipments, for the repair and maintenance of its products.⁸ See e.g. Optos, Inc., supra at 241 (“Defendants’ actions established a plausible threat of future [Optos] customer defections and the damages associated with those defections may escape accurate measurement”). Also, the resulting revenue loss or impact in sales would defy as well accurate quantification.

On the other side of the balance, there is no imaginable harm that would befall Philips PR if defendants were to publicly disclose or further disseminate plaintiff’s trade secret information for whatever financial or other competitive reasons. See American Health, Inc., supra at *6. To that end, the Court must naturally conclude that if plaintiff’s trade secret and/or confidential information were to be known or used by any competitor, both the value of its competitive advantage and goodwill – e.g. due to the inability of servicing returning customers – could be harmed beyond calculable and sustained economic repair. Id.

be under the obligation to prove irreparable damages”(Emphasis ours).

For this and the additional reasons stated above, the irreparable harm prong is satisfied. As is clear, defendants' attempts to obtain a "competitive edge" over Philips PR are unwarranted inasmuch as they are based on fraudulent representations, the unlawful entry into plaintiff's protected computer systems and misappropriation of its trade secrets. An injunction here would simply serve to prohibit defendants from using improperly obtained proprietary information; using, directing, aiding or conspiring with others to access plaintiff's proprietary computer systems; and further disseminating plaintiff's confidential information. As a result, Philips PR is entitled to injunctive relief under the local and federal statutes on which it relies.

C. Balance of Harms and Public Interest

The balance of harms weighs heavily in favor of granting Philips PR's request for injunctive relief. And that is because, to the extent that defendants suffer harm from the grant of injunctive relief, such harm results solely from their willful violations of the CFAA and ITSPA.

In balancing the prospective harms, a defendant's claim of irreparable harm should ring hollow when he/she decides to engage in improper conduct with knowledge of the potential consequences. Thus, the only harm an injunction would inflict upon defendants in the instant case would be to enjoin them from engaging in the intentional, malicious and/or willful conduct that they have directed at Philips PR's proprietary computer systems, and from further benefiting from their unlawful conduct. Put simply, illegal activities are not worthy of protection. See Century ML Cable Corp., *supra* at 173.

⁸ All this without considering that if defendants' conduct were not enjoined and/or held unlawful, other field service engineers to leave plaintiff in the future would be enticed to engage in similar conduct.

The public interest weighs heavily in favor of injunctive relief preventing defendants from engaging in conduct that is unlawful and detrimental to Philips PR. As alleged in its Complaint, when entering into contracts with hospitals and healthcare providers for the repair and maintenance of Philips medical equipments, defendants are misrepresenting that their computer systems are being accessed through legitimate purposes when, in fact, they are not. See Complaint, ¶67; see also e.g. CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 WL 715601, *7 (N.D. Ill. 2000)(holding that defendants' illegal sales of cable television "descramblers" were "against the public interest"). Thus, it can be logically concluded that the public has an interest in being protected from inducements to obtain services based on misappropriated trade secret information and deceptive methods. See American Health, Inc., *supra* at *7 ("Puerto Rico has a strong public interest in preserving the rights of its citizens against the misappropriation and misuse of their property").

THE COURT SHOULD SET A *DE MINIMIS* BOND

This Court should set a *de minimis* bond in this case. Pursuant to Fed. R. Civ. 65(c), the amount of security required for the issuance of a preliminary injunction is a matter that falls within the ample range of discretion of this Honorable Court. See Con. of Puerto Rico v. Price Commission, 342 F.Supp. 1308, 1309 (D.P.R. 1972); see also Fed. R. Civ. P. 65(c) ("The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained"). Here, Philips PR has sufficiently established that defendants have unlawfully accessed plaintiff's CSIP Digital Rights Management Application and Proprietary Service Applications without authorization; propagated their passwords and other security features;

and used its trade secrets for their own profit and financial benefit, in violation of applicable federal and state law.

Thus, plaintiff has set forth an overwhelming likelihood that it will prove the violations of the statutes under which it has brought this suit. Moreover, the issuance of an injunction – which, in essence, will only preclude defendants from continuing their illegal conduct – will not harm Mr. Sumpter López, Mr. Bracero, Mr. Toro nor GIS' business.⁹

In sum, the purpose of the injunctive relief Philips PR seeks is tailored to prevent defendants from engaging in any additional unlawful acts, and to prevent defendants from continuing to wrongfully benefit from its prior unlawful acts. In no legitimate sense will defendants be “harmed” if the injunctive relief requested by plaintiff is issued. Accordingly, this Court should keep the security amount as required by Fed. R. Civ. P. 65(c) to a minimum.

WHEREFORE, plaintiff Philips PR prays that this Court enter:

1. A preliminary injunction enjoining defendants from directly or indirectly:
 - a. trafficking Philips' Proprietary Service Applications along with their passwords and other security features;
 - b. using, directing, aiding or conspiring with others to access plaintiff's proprietary computer systems;
 - c. copying, reproducing, disseminating or using Philips' Proprietary Service Applications;
 - d. circumventing and/or assisting others to circumvent plaintiffs' technological measures in order to access its proprietary computer systems;

⁹ To the extent, of course, that defendants' business model does not solely rely on their illegal and unauthorized use of Philips PR's proprietary computer systems. In that case, any “harm” or “damage” which might ensue can only be described as the natural consequence of defendants knowingly and intentionally placing themselves in harm's way.

e. using plaintiff's trade secrets and/or confidential (proprietary) information for their own profit and financial benefit.

2. That the Court issue an Order directing defendants to preserve and maintain all records, in any form (either paper, electronic, or otherwise) that evidence, reference, concern, or relate, in any way to defendants' unlawful acts, as set forth in the Complaint.

3. That the Court issue an Order requiring defendants to file with the Court and to serve on counsel for plaintiff within thirty (30) days from the entry of the injunction a report in writing under oath, setting forth in detail the manner and form in which defendants have complied with the injunction and orders.

4. An award of such other and further relief as this Court deems appropriate under the circumstances.

RESPECTFULLY SUBMITTED.

WE HEREBY CERTIFY that on this same date, we electronically filed the foregoing with the Clerk of the Court using the CM/ECF system.

In San Juan, Puerto Rico, this 2nd day of November 2015.

ADSUAR MUÑIZ GOYCO
SEDA & PÉREZ-OCHOA, P.S.C.
P.O. Box 70294
San Juan, Puerto Rico 00936-8294
Tel: 787.756.9000 / Fax: 787.756.9010
Email: epo@amgprlaw.com
amercado@amgprlaw.com

/s/Eric Pérez-Ochoa
Eric Pérez-Ochoa
USDC-PR No. 206314

/s/Alejandro H. Mercado
Alejandro H. Mercado
USDC-PR No. 224708

*Counsel for Philips Medical
Systems Puerto Rico, Inc.*